

EX PARTE

January 14, 2010

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: Notice of Ex Parte Communication, GN Docket No. 09-191, WC Docket No. 07-52

Dear Ms. Dortch:

On January 12, 2010, Lauren Van Wazer, Cox Enterprises; Vint Cerf, Google; Gerard Lewis, Comcast; Dave Tennenhouse, New Venture Partners; David E. Young, Verizon; David Reed, MIT¹; Scott Jordan, UC Irvine; Paul Mankiewicz, Alcatel-Lucent; Gustavo de los Reyes, AT&T; Cathy Massey, Clearwire; Robb Topolski, New America Foundation; and Paul Kenefick, Alcatel-Lucent met with members of the Commission to discuss issues associated with the open Internet, and reasonable network management practices, focusing on methods that may be taken by service providers to deal with security threats and unwanted or unlawful transfers. This meeting was organized as part of the Technical Advisory Process (TAP), which was created to provide the Commission engineering guidance on network management issues for the Internet. FCC participants at the meeting included Julius Knapp, OET; Jon Peha, OSP; Zachary Katz, OSP; and Walter Johnston, OET. (A full list of meeting attendees is attached.)

The purpose of the meeting was to provide the Commission with general information on how service providers confront the issues of “security threats,” “unwanted content” and “unlawful transfers” in providing Internet service, and other services such as e-mail, to their end users and the potential impact such actions may have on users and upstream content and application providers. During the meeting, the term “unwanted content” was generally described as including such things as viruses, worms, Trojans and spam, while “security threats” included attacks on the some element of the network such as a distributed denial of service attack or an attack on the domain name system, and “unlawful transfers” was discussed as including unlawful content, such as child pornography, as well as unlawful transmissions of content, such as unlawful transfers of copyrighted materials.

It was noted that a service provider’s response to “unwanted content” may be dictated by the context in which it occurs. Participants explained that attacks on critical network

¹ David Reed and Scott Jordan participated in this meeting as subject matter experts and did not represent the universities with which they are associated.

resources may initiate an immediate, extensive, and adaptive response to the threat while other forms of unwanted content, *e.g.*, spam, are long-term events calling for a non-emergency or continual response that has evolved from the service provider's efforts in dealing with this specific form of unwanted content.

Participants noted that a valuable function is provided by various industry working groups such as the Messaging Anti-Abuse Working Group (MAAWG), which strive to summarize the experiences of service providers and others in dealing with unwanted content into industry "best practices." Due to the many-faceted nature of dealing with unwanted content, no single industry group covers all issues associated with best practices for dealing with unwanted content. Nevertheless, a number of groups discussed at the meeting such as the Internet Engineering Task Force (IETF) and the North American Network Operators Group (NANOG) play an important and ongoing role in addressing these and related issues in open, technical forums.

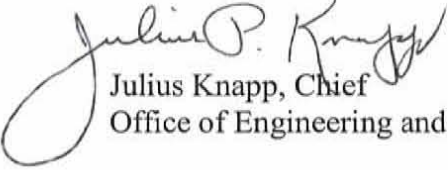
The issue of transparency in these matters was also discussed. Participants noted that methods and practices of the service providers that affect end users or applications that customers may be using should be disclosed in reasonable detail. Participants also noted that different kinds of information may be suitable for different audiences, such as basic information suitable for most consumers, more detailed information suitable for people with a technical background, and quite detailed technical information that would be helpful to applications developers. Other participants noted that this need for disclosure should be balanced against the need not to disclose information to originators of "unwanted content" that might assist them in breaching protective mechanisms that are in place.

During the course of the meeting, participants discussed the fact that the problem of "unwanted content" can be viewed from a network layered perspective and that mechanisms to deal with "unwanted content" may vary by layer (such as the application layer). Methods directed towards the source of unwanted content are appropriately quite different from methods taken to protect a specific recipient of unwanted content. The latter may be done at the request of the consumer (*e.g.* spam filters). The former may occur at the point of ingress to the network or within the network, and may be intended to protect the network and multiple consumers. Moreover steps taken by applications providers (*e.g.* email) are sometimes different from steps taken by IP access providers. Specific actions for various problems were presented from different perspectives. It was also recognized that the ability to detect unwanted or illegal content automatically is imperfect and that this should be a consideration in development of policies or methods. The participants emphasized that the development of such techniques and practices is and will continue to be an on-going process as the originators of unwanted content develop new techniques and the service providers respond.

Finally, participants noted that the response to "unlawful transfers" typically differs today from that for "unwanted content." In regard to copyrighted material, the approach within the United States, in general, is to work cooperatively with those claiming copyright violations when validly requested to do so under the Digital Millennium Copyright Act.

and to notify end users associated with such infringements to make them aware of the legal concerns regarding their actions. Beyond copyright infringement, standard policies exist among service providers for processing and responding to valid law enforcement requests such as subpoenas, warrants, and court orders.

Given the complexity of services, applications, and content provided over the Internet and managed IP networks today, it was suggested that it would be valuable to have technical definitions for the different service offerings and in particular the definition of what constitutes an Internet access service. The next meeting in the TAP will discuss reasonable network management as it relates to quality of service.



Julius Knapp, Chief
Office of Engineering and Technology

Attendees

Name	Organization
Stephen Buenzow	FCC
Vint Cerf	Google
Michael Goldstein	FCC
Richard Hovey	FCC
Scott Jordan	UC Irvine
Paul Kenefick	Alcatel-Lucent
John Kiefer	FCC
Julius Knapp	FCC
Gerard Lewis	Comcast
Paul Mankiewicz	Alcatel-Lucent
Cathy Massey	Clearwire
Alison Neplokh	FCC
Stagg Newman	FCC
Jon Peha	FCC
David P. Reed	Self (MIT Media Lab)
Gustavo de los Reyes	AT&T
Dave Tennenhouse	New Venture Partners
Robb Topolski	New America Foundation
Lauren Van Wazer	Cox Enterprises
John Wong	FCC
David Young	Verizon